# SSH與ESXi 6.7P04(內部版本17167734)及更高版本不相容

## 目錄

# 簡介

HXDP [3.5(x), 4.0(x)]和ESXi 6.7P04(內部版本17167734)及更高版本之間存在軟體互操作性問題。 客戶應避免這種軟體組合。

**附註：此問題擴展至高於6.7P04的任何6.7 ESXi版本**

**HXDP 4.0(2e)中解決了相容性問題。 此問題不會影響HXDP 4.5(1a)及更高版本。**

## 需求

ESXi 6.7P04(內部版本17167734及更高版本

HXDP版本 — 3.5(x)、4.0(x)

## 更多資訊

### 缺陷

相關錯誤ID為 CSCvv88204 **- ESXi OpenSSH與HXDP的互操作性問題**

此問題發生在ESXi 6.7P04中，原因是VMware將openSSH庫升級到：OpenSSH_8.3p1。此新版本的OpenSSH取消了HXDP在直接通過SSH與ESXi通訊時內部使用的金鑰交換方法的支援。下面是OpenSSH changelog中的一個片段，其中描述了在該版本中所做的重大更改：

```
ssh(1), sshd(8): this release removes diffie-hellman-group14-sha1 from the default key exchange
proposal for both the client and server.
```

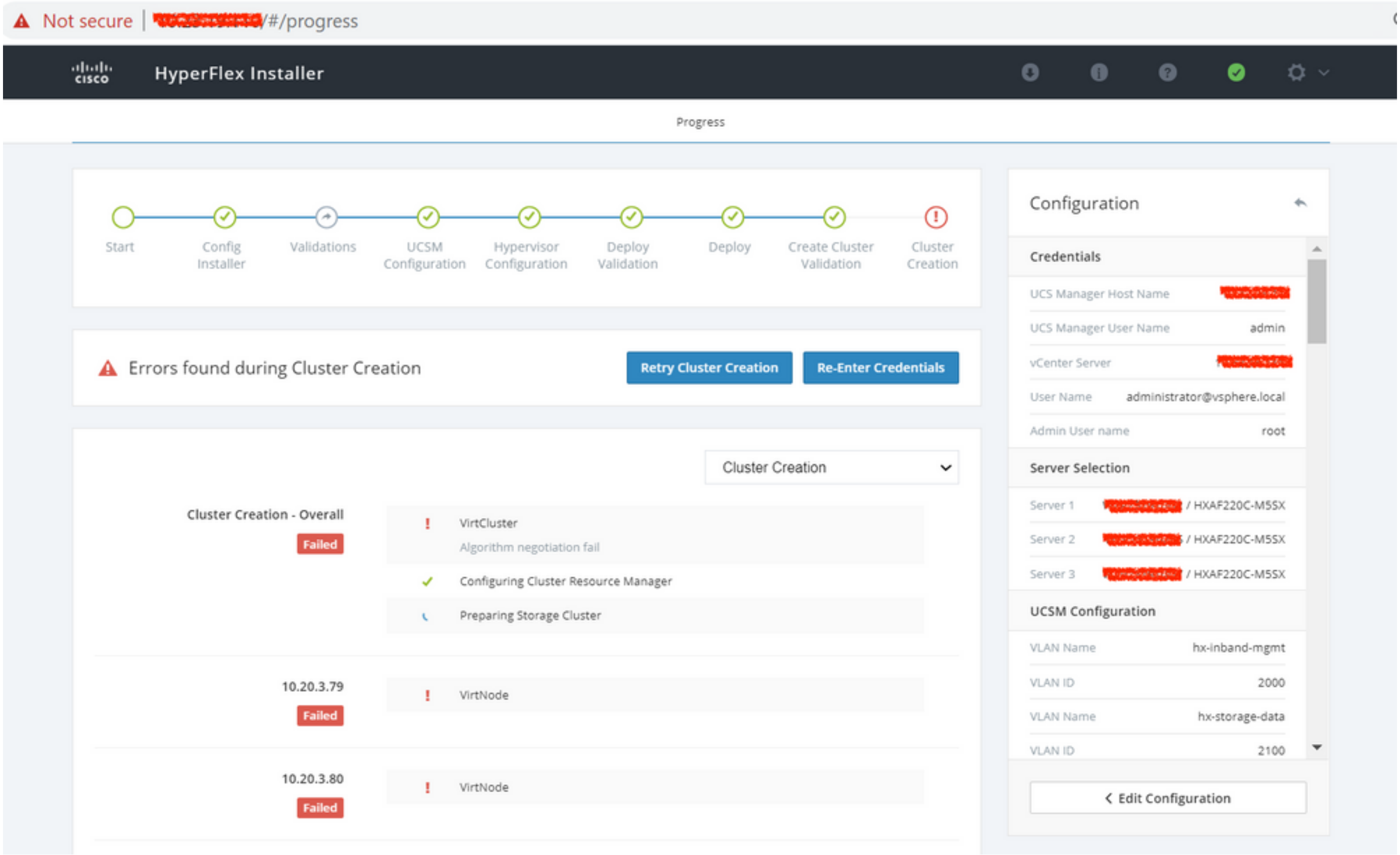
### 軟體諮詢

有關更多詳細資訊，請參閱軟體諮詢 — Cisco ESXi 6.7 P04軟體諮詢

## 受影響區域

HX的一些功能領域將受到影響，包括：

- 新建群集(可能會因演算法協商**失敗而失敗**)



Errors found during Cluster Creation

Cluster Creation - Overall
Failed
! VirtCluster
Algorithm negotiation fail
✓ Configuring Cluster Resource Manager
Preparing Storage Cluster

10.20.3.79
Failed
! VirtNode

10.20.3.80
Failed
! VirtNode

Configuration

Credentials

| | |
|---|---|
| UCS Manager Host Name | [redacted] |
| UCS Manager User Name | admin |
| vCenter Server | [redacted] |
| User Name | administrator@vsphere.local |
| Admin User name | root |

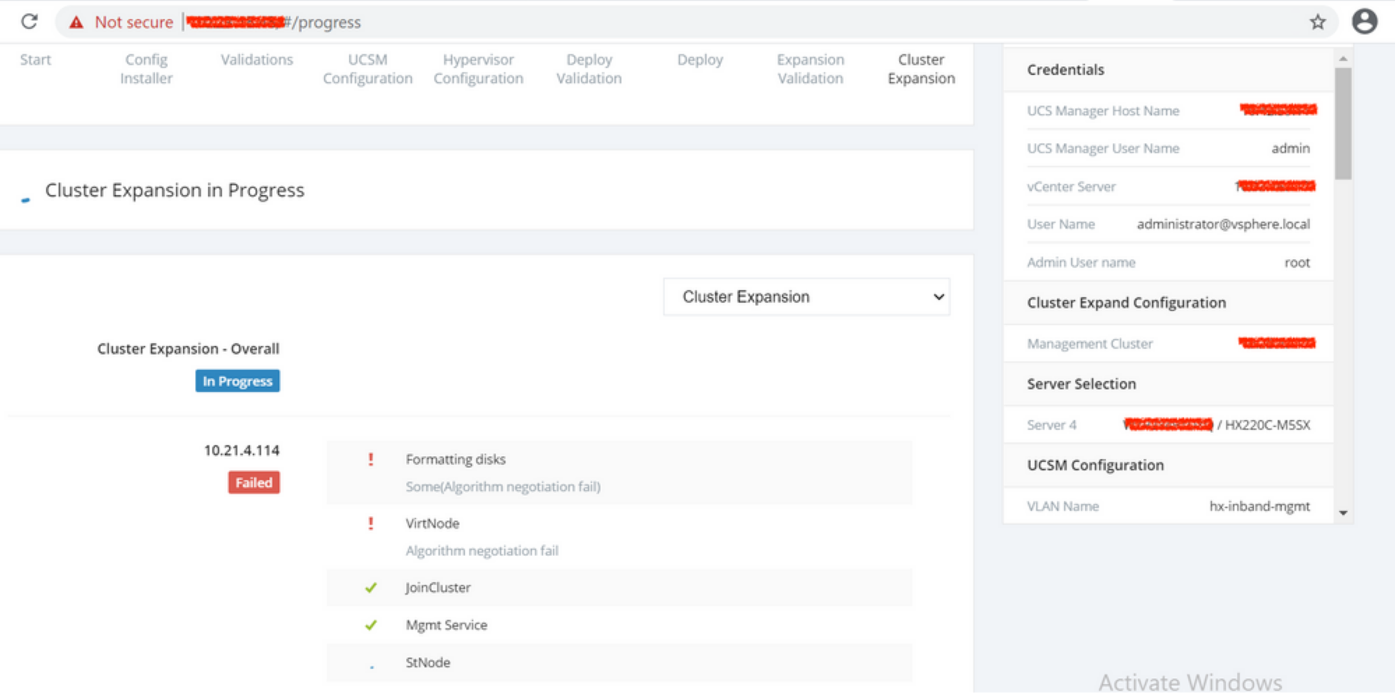
Server Selection

| | |
|---|---|
| Server 1 | [redacted] / HXAF220C-M5SX |
| Server 2 | [redacted] / HXAF220C-M5SX |
| Server 3 | [redacted] / HXAF220C-M5SX |

UCSM Configuration

| | |
|---|---|
| VLAN Name | hx-inband-mgmt |
| VLAN ID | 2000 |
| VLAN Name | hx-storage-data |
| VLAN ID | 2100 |

- 群集擴展(可能失敗，但演算法**協商失敗**)



Cluster Expansion in Progress

Cluster Expansion - Overall
In Progress

10.21.4.114
Failed
! Formatting disks
Some(Algorithm negotiation fail)
! VirtNode
Algorithm negotiation fail
✓ JoinCluster
✓ Mgmt Service
StNode

Credentials

| | |
|---|---|
| UCS Manager Host Name | [redacted] |
| UCS Manager User Name | admin |
| vCenter Server | [redacted] |
| User Name | administrator@vsphere.local |
| Admin User name | root |

Cluster Expand Configuration

| | |
|---|---|
| Management Cluster | [redacted] |

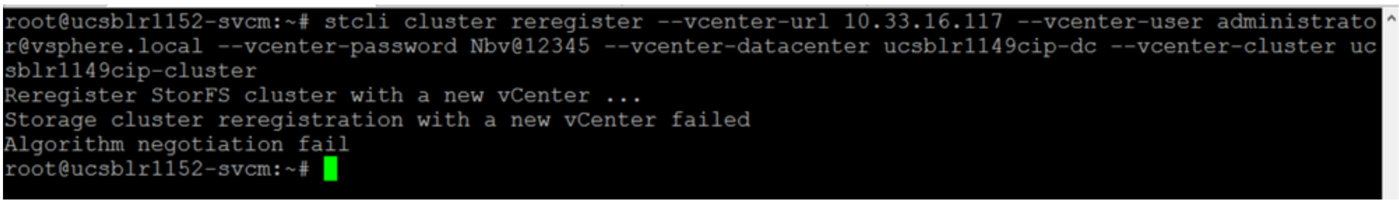
Server Selection

| | |
|---|---|
| Server 4 | [redacted] / HX220C-M5SX |

UCSM Configuration

| | |
|---|---|
| VLAN Name | hx-inband-mgmt |

- 群集重新註冊(stcli群集重新註冊可能失敗，並且**「演算協商失敗」**)



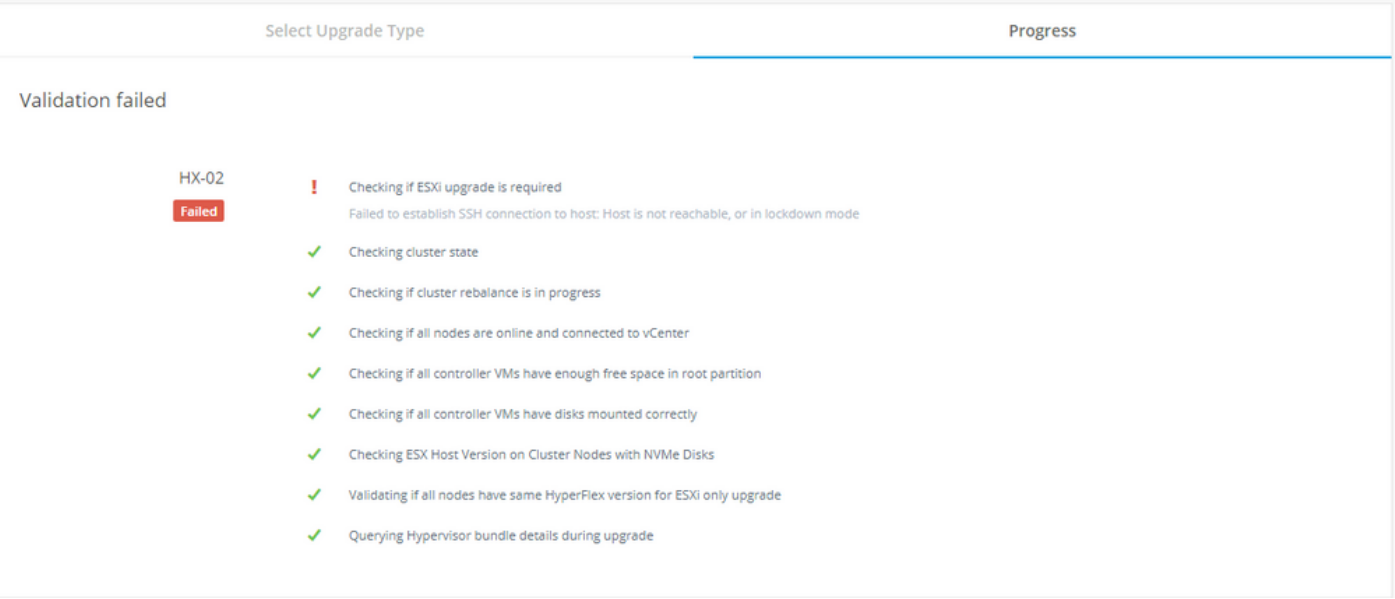
```
root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrato
r@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster uc
sblr1149cip-cluster
Reregister StorFS cluster with a new vCenter ...
Storage cluster reregistration with a new vCenter failed
Algorithm negotiation fail
root@ucsblr1152-svcm:~# 
```

- HX Connect中的系統資訊頁面
- 升級可能會失敗，**出現「Failed to Establish SSH Connection to host」**或**「Errors found during upgrade」**

ESXi升級失敗，出現ssh異常 —

2020-12-16-10:31:04.675 [] [] [vmware-upgrade-pool-9]錯誤c.s.sysmgmt.stMgr.SshScpUtilImpl — 無法建立到主機的SSH連線：主機無法連線或處於封鎖模式

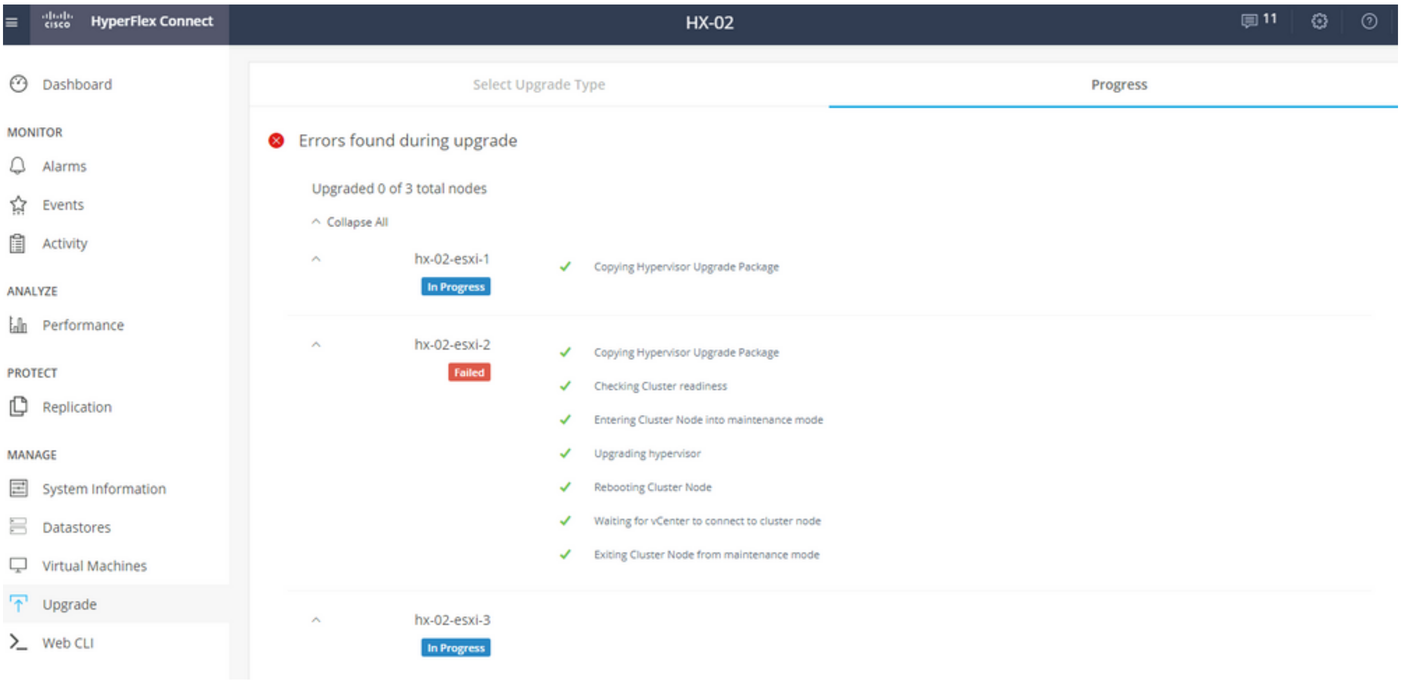
com.jcraft.jsch.JSch異常：演算法協商失敗



Validation failed

HX-02
Failed

! Checking if ESXi upgrade is required
Failed to establish SSH connection to host: Host is not reachable, or in lockdown mode
✓ Checking cluster state
✓ Checking if cluster rebalance is in progress
✓ Checking if all nodes are online and connected to vCenter
✓ Checking if all controller VMs have enough free space in root partition
✓ Checking if all controller VMs have disks mounted correctly
✓ Checking ESX Host Version on Cluster Nodes with NVMe Disks
✓ Validating if all nodes have same HyperFlex version for ESXi only upgrade
✓ Querying Hypervisor bundle details during upgrade



Errors found during upgrade

Upgraded 0 of 3 total nodes

Collapse All

hx-02-esxi-1
In Progress
✓ Copying Hypervisor Upgrade Package

hx-02-esxi-2
Failed
✓ Copying Hypervisor Upgrade Package
✓ Checking Cluster readiness
✓ Entering Cluster Node into maintenance mode
✓ Upgrading hypervisor
✓ Rebooting Cluster Node
✓ Waiting for vCenter to connect to cluster node
✓ Exiting Cluster Node from maintenance mode

hx-02-esxi-3
In Progress

- 潛在的其他領域

# 因應措施

HXDP發行說明已更新，專門指出此版本的6.7在3.5(x)和4.0(x)版本上不受支援。此問題已在HXDP 4.0補丁 — 4.0(2e)和所有版本4.5(1a)及更新版本中修正。

- 使用ESXi中內建的回滾機制回滾到相容的ESXi版本。
- 另一種可能的解決方法是通過在每個ESXi主機上更新sshd_config並重新啟動SSH服務來重新啟用已移除的金鑰交換方法。建議僅臨時實施此解決方法。

**注意：**目標應該是將群集移至固定HXDP版本，並儘快刪除此解決方法。如果將此額外金鑰演算法設定新增到sshd_config，群集不應長期處於此狀態。

## 解決方法的步驟

如果無法將HXDP升級到固定版本，請使用以下解決方法 —

### 解決方法1

- 使用ESXi中內建的回滾機制回滾到相容的ESXi版本。請參閱vmware KB - https://kb.vmware.com/s/article/1033604

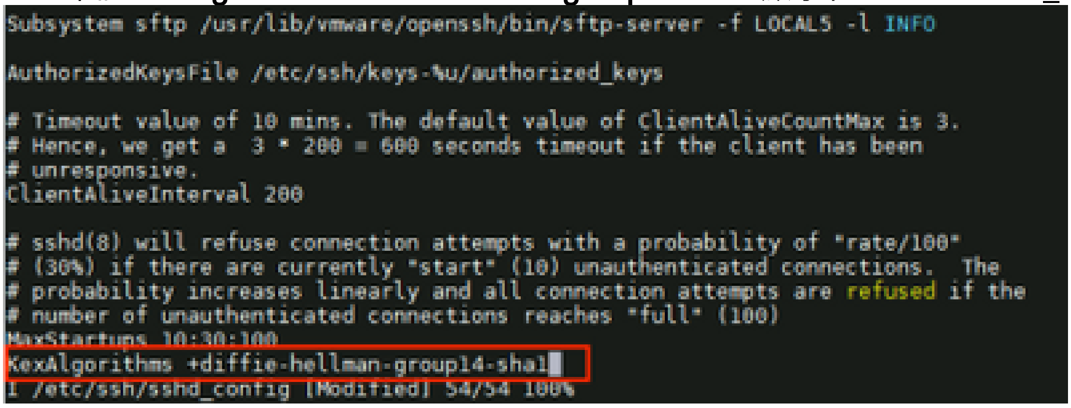
### 解決方法2

通過在每個ESXi主機上更新sshd_config並重新啟動SSH服務，重新啟用已移除的金鑰交換方法。

- 將+diffie-hellman-group14-sha1新增到每個ESXi主機上的/etc/ssh/sshd_config下的KexAlgorithms中

```
# echo "KexAlgorithms +diffie-hellman-group14-sha1" >> /etc/ssh/sshd_config
```

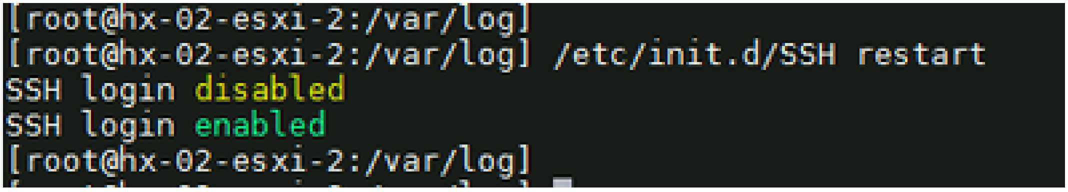
- 確認**KexAlgorithms +diffie-hellman-group14-sha1**顯示在/etc/ssh/sshd_config中



```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO

AuthorizedKeysFile /etc/ssh/keys-%u/authorized_keys

# Timeout value of 10 mins. The default value of ClientAliveCountMax is 3.
# Hence, we get a  3 * 200 = 600 seconds timeout if the client has been
# unresponsive.
ClientAliveInterval 200

# sshd(8) will refuse connection attempts with a probability of "rate/100"
# (30%) if there are currently "start" (10) unauthenticated connections.  The
# probability increases linearly and all connection attempts are refused if the
# number of unauthenticated connections reaches "full" (100)
MaxStartups 10:30:100
KexAlgorithms +diffie-hellman-group14-sha1
1 /etc/ssh/sshd_config [Modified] 54/54 100%
```

- 重新啟動ESXi SSH進程

```
# /etc/init.d/SSH restart
```



```
[root@hx-02-esxi-2:/var/log]
[root@hx-02-esxi-2:/var/log] /etc/init.d/SSH restart
SSH login disabled
SSH login enabled
[root@hx-02-esxi-2:/var/log] _
```

- 重新啟動或繼續以前失敗的工作流。